February 1, 2001

INSPECTOR GENERAL INSTRUCTION 4630.1

SUBJECT: Electronic Mail Policy

References: See Appendix A.

A. Purpose. This Instruction updates the Office of the Inspector General, Department of Defense (OIG, DoD), Electronic Mail (E-Mail) policy.

B. Cancellation. This Instruction supersedes IGDINST 4630.1, *Electronic Mail Policy*, May 18, 2000.

C. Applicability and Scope. This Instruction applies to the Offices of the Inspector General; the Deputy Inspector General; the Assistant Inspectors General; Director, Administration and Information Management; Director, Departmental Inquiries; Director, Intelligence Review and the Office of the Deputy General Counsel (Inspector General), which is provided support by the OIG, DoD, when its Office of the Secretary of Defense-provided equipment interfaces with the OIG, DoD, network. For purposes of this Instruction, these organizations are referred to collectively as OIG components.

D. Definitions. See Appendix B.

E. Policy

1. The OIG, DoD, shall not transfer classified data, as defined in references b, c, and d via E-Mail without approval of the Designated Approving Authority (DAA). All classified data transfers shall be performed only on accredited, classified systems.

2. In accordance with guidance provided by the Chief Information Officer Council, Government office equipment, including E-Mail, shall only be used for official purposes, except as specifically authorized in this Instruction. Employees are permitted limited appropriate use of Government office equipment for personal needs if the use does not interfere with official business and involves minimal additional expense to the Government. This limited personal use of Government office equipment should take place during the employee's non-work time. This privilege to use Government office equipment for non-Government purposes may be revoked or limited at any time. This personal use must not result in loss of employee productivity or interference with official duties. Moreover, such use should incur only minimal additional expense to the Government in areas, such as:

   a. Communications infrastructure costs; e.g., telecommunications traffic, etc.

   b. Use of consumables in limited amounts; e.g., paper, ink, toner, etc.

   c. General wear and tear on equipment.

   d. Data storage on storage devices.

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
01 Feb 2001	N/A	-

Title and Subtitle Electronic Mail Policy	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-2884	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 8	

e. Transmission impacts with moderate E-Mail message sizes, such as E-Mail with attachments smaller than 10 megabytes.

3. This policy in no way limits employee use of Government office equipment, including Information Technology (IT), for official activities.

4. It is the responsibility of employees to ensure that their personal use of Government office equipment is not falsely interpreted to represent the agency. If there is an expectation of such an interpretation, a disclaimer must be used, such as "The contents of this message are mine personally and do not reflect any position of the Government or my agency."

5. Employees do not have a right, nor should they have an expectation, of privacy while using any Government office equipment or systems at any time, including using E-Mail. To the extent that employees wish that their private activities remain private, they should avoid using office equipment or systems for personal E-Mail. By using Government office equipment or systems, employees imply their consent to disclosing the contents of any files or information maintained or passed through Government office equipment. By using office equipment or systems, consent to monitoring and recording is implied with or without cause, including (but not limited to) using E-Mail. Any use of Government E-Mail is made with the understanding that such use is generally not secure, private or anonymous and may be monitored at any time.

6. Employees shall download E-Mail attachments and files to a diskette whenever possible and check for viruses before they expose OIG, DoD, computers to this electronic information. If the file is too large to download to a floppy diskette, the employee shall check for viruses before opening the file from the hard disk.

7. Employees shall not send copyrighted graphics or documents through E-Mail without the owner's permission.

8. Use other than described herein is misuse of information resources.

9. It is a violation of regulations to use Government equipment for personal gain.

10. The OIG, DoD, E-Mail standard is determined by the Chief Information Officer (CIO) as specified in reference a.

11. End users shall send and receive Internet E-Mail messages only through procedures specified in paragraph G.

12. E-Mail messages, like all electronic documents, are considered agency records and are subject to the provisions of references f, g, and h.

13. Many personal E-Mail programs now allow "instant messaging" or are web-enabled, which allows access via any Internet connection. Accessing or logging onto web-enabled personal E-Mail services, or using "instant messaging," via the OIG, DoD, network impacts on communication capacity and weakens OIG, DoD, network defenses. Web-enabled E-Mail services and "instant messaging" bypass OIG, DoD, virus protection. Therefore, users are not authorized to use OIG, DoD, resources to access web-enabled personal E-Mail services or "instant messaging" without the express permission of the ISD.

14. Users may not use personal E-Mail services for official business without the express permission of the ISD.

15. Failure to adhere to the provisions of this Instruction may result in termination of access to all OIG, DoD-supported local area networks and in other disciplinary and legal penalties, as appropriate.

F. Responsibilities

1. With regard to OIG, DoD, E-Mail accounts, **End Users** shall:

a. Check for messages regularly.

b. Dispose of messages (which may include filing, archiving, or deleting) before mailboxes become too full to receive additional correspondence, keeping in mind that E-Mail is subject to the provisions of references f, g, and h.

c. Use the E-Mail system only for its intended purpose and protect the security of information in accordance with references b through j.

d. Locate Internet addresses of intended message recipients. There is no comprehensive on-line directory of addressees available.

e. Provide their Internet address to those who wish to send them messages.

f. Scan all incoming attachments to Internet messages before introducing them into the OIG environment. See paragraph G for required procedure.

g. Dispose of unsolicited messages, such as advertisements, chain letters, jokes, etc., in accordance with the spirit of reference e. Further distribution of these types of messages is rarely in the spirit of reference e.

h. Refrain from any practices that might jeopardize, compromise, or render useless any OIG, DoD, data, system or network.

i. Be individually responsible and liable for any disclosures of personal information if the employee chooses to send such information through an electronic communications system provided by the OIG, DoD, or Federal Government, or both.

j. Not send secure, sensitive, classified, or potentially compromising information through an electronic communications system provided by the OIG, DoD, or Federal Government, or both unless approved by the DAA. All classified data transfers shall be performed only on accredited, classified systems. Information subject to references g and h shall be appropriately marked FOUO if transmitted electronically.

k. Refrain from any activities that could congest or disrupt an electronic communications system provided by the OIG, DoD, or Federal Government, or both.

l. Refrain from any inappropriate personal uses, including accessing personal E-Mail.

m. Store important E-Mail messages.

2. The **OIG Component Heads** shall ensure that the provisions of this Instruction and references a through j are implemented.

3. The **Personnel and Security Directorate (PSD), Office of Administration and Information Management (OA&IM),** shall:

a. Develop E-Mail security policies, standards, and procedures.

b. Ensure E-Mail use complies with applicable security laws, guidelines, regulations, and standards, both internal and external. That includes, but is not limited to, public laws and OIG, DoD, General Services Administration and Office of Management and Budget publications.

c. Make decisions on and assist end users with security safeguards for E-Mail use.

d. Advise and assist management on appropriate administrative action(s) if misuse occurs.

e. Perform duties delegated by the DAA.

4. The **Information Systems Directorate (ISD), OA&IM,** shall:

a. Manage the OIG, DoD, E-Mail system.

b. Establish and keep current internal lists and other internal addresses, including deleting the mailboxes of departed employees or those who have violated the provisions of this Instruction.

c. Support OIG, DoD, E-Mail users.

d. Monitor the use of electronic communications to ensure adequate performance and proper use, as approved by the CIO.

e. Use or disclose information obtained during the monitoring process only as required in the performance of official duties.

f. Notify the end user, the end user's manager, and the PSD of any problem concerning the end user's conduct in accessing and using E-Mail.

5. The **Administration and Logistics Services Directorate, OA&IM,** shall assist and advise when E-Mail messages constitute records subject to the provisions of references f, g, and h.

6. The **Inspector General, DoD,** shall designate the DAA and the CIO.

G. Procedures

1. End users must check for viruses that may accompany files transferred through E-Mail. Protection from viruses includes downloading the files to diskettes, whenever possible, and scanning before placing files on the hard drive. If users must decompress files, they must perform a second virus check of the decompressed files. If the file is too large to download onto a diskette, the user must check for viruses before executing or opening the file from the hard disk.

2. If the end user introduces any software, including that attached to E-Mail, into the OIG, DoD, environment that the ISD did not issue, the user is responsible for it. This includes any effect that the software may have on the operation of standard hardware and software. Even virus-free software may cause conflicts. If the ISD determines that software introduced by the user is causing a malfunction of standard hardware or software, the ISD shall return the user to the standard configuration. The ISD shall not assume responsibility for any functionality lost by a return to

standard configuration. The user is also responsible for operating the software within established laws, guidelines and procedures, including software licensing agreements.

H. Effective Date and Implementation. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

/signed/
Joel L. Leson
Director
Office of Administration
and Information Management

2 Appendices - a/s

APPENDIX A
REFERENCES

a. IGINST 7950.2, Microcomputer Hardware and Software Management Program, May 23 2000.

b. IGINST 5200.40, Security Requirements for Automated Information Systems, July 20, 2000.

c. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988.

d. DoD 5200.28-M, "ADP Security Manual," January 1973.

e. DoD 5500.7-R, "Joint Ethics Regulation (JER)," August 1993, as changed.

f. IGDM 5015.1, Records Management Program, October 25, 1994.

g. DoD 5400.7, DoD FOIA Program, September 1988.

h. DoD 5400.11-R, DoD Privacy Program, August 1983.

i. DoD Directive 5500.7, "Standards of Conduct," August 30, 1993.

j. DoD Directive 8000.1, "Defense Information Management (IM) Program," October 27, 1992.

APPENDIX B
DEFINITIONS

a. **Chief Information Officer.** The senior official appointed by the Inspector General, DoD, who is responsible for developing and implementing information resources management in ways that enhance OIG, DoD, mission performance through the effective, economic acquisition and use of information. The CIO is currently the Director of A&IM.

b. **Employee Non-Work Time.** Times when the employee is not otherwise expected to be addressing official business. Employees may, for example, use Government office equipment during off-duty hours, such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if the employee's duty station is normally available at such times).

c. **Inappropriate Personal Uses.** Employees are expected to conduct themselves professionally in the workplace and to refrain from using Government office equipment for activities that are inappropriate. According to the CIO Council, misuse or inappropriate personal use of Government office equipment includes, but is not limited to:

1. Any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment. For example, greeting cards, video, sound, or other large file attachments can degrade the performance of the entire network.

2. The creation, copying, transmission or retransmission of chain letters or other unauthorized mass mailings, regardless of the subject matter.

3. Using Government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

4. Use for commercial purposes or in support of "for-profit" activities or in support of other outside employment or business activity (e.g., consulting for pay, sales, or administration of business transactions, sale of goods or services) or for personal gain.

5. Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.

6. Use for posting agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government employee, unless appropriate agency approval has been obtained, or uses at odds with the agency's mission or positions.

7. Any use that could generate more than minimal additional expense to the Government.

8. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data that includes privacy information, copyrighted, trade marked, or material with other intellectual property rights (beyond fair use), proprietary data or export controlled software or data.

d. **Designated Approving Authority (DAA).** The official designated by the Inspector General, DoD, who has the authority to decide on accepting the security safeguards prescribed for an

information system. The DAA issues an accreditation statement that records the decision to accept those standards. The DAA is currently the Director of A&IM.

e. **Electronic Mail (E-Mail).** A means of communication that uses computer-to-computer data transfer technology, normally as textual messages or attached files.

f. **End-User.** An OIG, DoD, employee who uses automated equipment to perform work-related tasks.

g. **Internet.** The loosely connected worldwide collection of computer systems that uses a common set of communications standards to send and receive electronic information.

h. **OIG Environment.** Any computer, media, or network used by the OIG, DoD.

i. **Personal Use.** Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. Employees may make limited use under this policy of Government office equipment to seek employment in response to Federal Government downsizing or communicate with a volunteer charity organization.

j. **Privilege.** In the context of this policy, privilege means that the Executive Branch of the Federal Government is extending the opportunity to its employees to use Government property for personal use in an effort to create a more supportive work environment. However, this policy does not create the right to use Government office equipment for non-Government purposes. Nor does the privilege extend to modifying such equipment, including loading personal E-Mail software or making configuration changes. Government office equipment, including the E-Mail system, includes, but is not limited to, personal computers and related peripheral equipment and software, office supplies, Internet connectivity, and access to Internet services and E-Mail.

k. **Support.** Diagnosing and resolving problems regarding operating and using E-Mail.